

**Sources Sought Notice:**  
**National Data Warehouse**  
**Centers for Medicare & Medicaid Services**

This is a SMALL BUSINESS SOURCES SOUGHT notice. This is NOT a solicitation for proposals, proposal abstracts, or quotations. The purpose of this notice is to obtain information regarding: (1) the availability of qualified small business sources who either have or have the capability of obtaining a CMMI Level III certification or greater by time of award (anticipated May 2016); (2) whether they are small businesses; HUBZone small businesses; service-disabled, veteran-owned small businesses; 8(a) small businesses; veteran-owned small businesses; woman-owned small businesses; or small disadvantaged businesses; and (3) their size classification relative to the North American Industry Classification System (NAICS) code **541512 – Computer Systems Design Services**. Your responses to the information requested will assist the Government in determining the appropriate acquisition method, including whether a set-aside is possible. An organization that is not considered a small business under the applicable NAICS code should not submit a response to this notice.

**BACKGROUND**

The Centers for Medicare & Medicaid Services (CMS) purchases health care for an estimated 79 million people through Medicare and Medicaid. On behalf of these beneficiaries, CMS works to ensure high quality health care at a reasonable price and to provide information about benefits, health promotion, and choices. CMS is responsible for accurate, timely, relevant, understandable, and easily accessible information that will help beneficiaries evaluate health plan options, nursing home options, and make decisions on their individual health care needs. The Centers for Medicare & Medicaid Services (CMS) is required to broadly disseminate information to people with Medicare (and prospective people with Medicare), as well as, consumers in the Federally Facilitated Marketplace (FFM). CMS provides a broad range of information including the coverage options available, prescription drug information and General Medicare & Healthcare information.

In order to meet national program missions and strategies as well as legislative mandates (Balanced Budget Act of 1997 and Medicare Modernization Act of 2003), CMS operates a toll-free, nation-wide, 24x7x365 contact center with multiple sites to provide customer service and address inquiries. In addition to this, with new reform and regulations, and with the implementation of the Affordable Care Act (ACA), calls and inquiries also include issues regarding the Affordable Care Act (ACA), consumer health choices or other Federal programs and Department of Health and Human Services (DHHS) initiatives.

A key component of the Federally Facilitated Marketplace and Customer Contact Center, collectively known as the Contact Center Operations (CCO) is the National Data Warehouse (NDW). The NDW performs a significant role with oversight and monitoring functions under the Virtual Call Center Strategy (VCS) initiative and Medicare Reform legislation. The NDW acts as the central repository for capturing, aggregating, and analyzing information related to the beneficiary experience with Medicare and the consumer experience with Marketplaces. The NDW also serves as a foundation for operational and management reporting to support improved decision-making, business practices, and services to callers. The data stored in the NDW is used

to monitor, forecast, trend, analyze, and report on the performance of the CCO contract and all channels of communication available to Medicare Beneficiaries and Marketplace Consumers.

The data includes information for CMS' Virtual Contact Center operations including, but not necessarily limited to:

- Workforce management data
- Desktop activity
- TTY/TDD
- Quality monitoring
- Print fulfillment
- Medicare disenrollments
- Reference center escalations
- Beneficiary satisfaction surveys
- IVR data
- Web Chat metrics
- Feedback tool
- Genesys/ACD information

## **CAPABILITY STATEMENT INFORMATION**

Please prepare a **Capability Statement** addressing your knowledge, expertise and experience, within the last three (3) years, for each of the following capabilities/requirements. The offeror shall demonstrate experience with contracts of similar size and scope. Include the following information for each reference utilized to demonstrate experiences and capabilities:

- Name of Contracting Activity
- Contract Number
- Period of Performance
- Total contract value
- A detailed description of how the reference demonstrates the experience and capabilities required to include how the experience is similar in size and scope to this effort. If you were a subcontractor versus the prime contractor please describe in detail your specific role in contract performance.
- Contracting Officer and telephone
- Customer's Program Manager and telephone

### **Capabilities/Requirements:**

1. Demonstrate your experience in providing 24x7x365 operations for a large, complex, highly scalable data center requiring strict Service Level Agreements (SLAs). Uptime on this system must be 99.0% or better. Furthermore, demonstrate your experience in providing professional staff full time equivalents (FTEs) to run, manage and oversee data center operations with the ability to develop, deliver, maintain and adhere to structured project management plans based on integrated project schedules incorporating interdependencies among a network of complex program areas.
2. Demonstrate your experience in data management architecture and architecture development strategies that align to the overall NDW Functional Requirements of this task (see p. 6).
3. Demonstrate your expertise and experience with Business Intelligence (BI) tools, architecture, and data mining complex data feeds. Include specific experience and expertise in using Informatica™, Microstrategy™ and IBM Cognos™ databases and provide examples of complex data architecture work within the last 3 years.
4. Explain and provide examples of your experience with and expertise in change management processes, specific to enterprise level operations, to include developing, documenting & maintaining run books for reporting capabilities in an aggressive update schedule. Specifically show competency in managing large-scale, complex project collaborations between your company and other business stakeholders.
5. Demonstrate your experience with scalability and security in protecting data and information with customer, person-sensitive information including Personal Health Information and Personally Identifiable information (personal health records, etc.). Specifically address experience and expertise with security standards maintaining Federal Information Security Management Act (FISMA) compliant system(s). Be sure to document experiences and expertise reflecting 3-zone architecture, Section 508 compliancy, and aligning factors represented in the CMS Technical Reference Architecture (TRA). (<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/Technical-Reference-Architecture-Standards/index.html>)

6. Demonstrate your experience and capabilities in providing a quality process end-to-end with improvement results as well as the process you have used to ensure quality and adherence (Accuracy, Completeness, etc.) across multiple data sources and channels.
7. Provide your current CMMI level certification. If not already CMMI Level III certified or greater, demonstrate your ability to achieve this certification level by the anticipated date of award of May, 2016. Please describe your specific plan to include a timeline.
8. Discuss any concerns regarding the difficulty and/or feasibility of the proposed acquisition, possible solutions and approaches that may currently exist in the marketplace, and information regarding innovative ideas or concepts.

#### **ADDITIONAL INFORMATION REQUESTED:**

Interested parties having the capabilities necessary to perform this requirement may submit capability statements via email to Ryan Kaufman ([ryan.kaufman@cms.hhs.gov](mailto:ryan.kaufman@cms.hhs.gov)).

CAPABILITY STATEMENTS MUST DEMONSTRATE THE MINIMUM REQUIREMENTS OUTLINED ABOVE. Please address each in the order listed above under “Capability Statement Information.”

Capability Statements shall be limited to 20 pages and shall also include the following information:

Business Information --

- a. DUNS
- b. Tax ID
- c. Company Name
- d. Company Address
- e. Company Point of Contact, Phone and Email address
- f. Current GSA Contracts and Schedules
- g. Do you have a Government approved accounting system? If so, please identify the agency that approved the system.
- h. Business Size Status (e.g., small business, 8(a), woman owned, veteran owned, etc.) as validated via the Small Business Administration for the applicable NAICS code **541512 – Computer Systems Design Services** (Size Standard - \$27.5 Million). Additional information on NAICS codes can be found at [www.sba.gov](http://www.sba.gov).
- i. Point of Contact, Phone and Email address of individuals who can verify the demonstrated capabilities identified in the responses.

The Capability Statement shall designate any/all teaming arrangements and the work proposed to be performed by each team member. Specifically, the Capability Statement must address how much of the effort would be performed by any proposed team member. Note that any resulting small business set aside would require that at least 50% of the cost of contract performance for personnel to be expended for employees of the concern (See FAR 52.219-14, Limitations on Subcontracting).

**Responses must be submitted on or before ~~Tuesday, January 6, 2015~~ Monday, January 19, 2015.** Capability statements will not be returned and will not be accepted after the due date. This notice does not obligate the Government to award a contract or otherwise pay for the information provided in response. The Government reserves the right to use information provided by respondents for any purpose deemed necessary and legally appropriate. Any organization responding to this notice should ensure that its response is complete and sufficiently detailed to allow the Government to determine the organization's qualifications to perform the work. Respondents are advised that the Government is under no obligation to acknowledge receipt of the information received or provide feedback to respondents with respect to any information submitted. After a review of the responses received, a pre-solicitation synopsis and solicitation may be published in Federal Business Opportunities. However, responses to this notice will not be considered adequate responses to any solicitation.

**Confidentiality.** No proprietary, classified, confidential, or sensitive information should be included in your response. The Government reserves the right to use any non-proprietary technical information in any resultant solicitation(s).

Questions concerning submission requirements may be directed to Ryan Kaufman, Contract Specialist, 410-786-2353 or [ryan.kaufman@cms.hhs.gov](mailto:ryan.kaufman@cms.hhs.gov). CMS will not entertain questions related to contracting strategy.

## **Functional Requirements and Resource Capability Overview**

The following provides potential responders with an overview of the types of support that would be required of the NDW contractor. Note that although this is an extensive list, it is not meant to be all inclusive.

### **A. NDW Functional Requirements:**

#### **The Contractor Shall:**

1. Perform data collection from multiple operational source systems, and, data enrichment and integration, to ensure that the required data elements appropriately populate the single, web-based information data store.
2. Provide and maintain an operational data center environment to host the Development, Test, and User acceptance Testing (UAT) of NDW environments only.
3. Provide the necessary access, information, and assistance to CMS and other CMS contractors utilizing the system.
4. Provide an infrastructure with redundant power; heat, ventilation, and air conditioning (HVAC); fire suppression systems; secure entry management systems; and building management services. (Physical Environment control family)
5. Be responsible for identifying and communicating to the Virtual Data Center (VDC) Contractor any special requirements for support of the NDW application. The production environment is currently located at the Companion Data Services' VDC. The VDC Contractor is responsible for hosting the NDW application in the VDC, including the daily operations of networking, operating systems, hardware, and other maintenance activities.
6. Provide necessary premise-based network-communications equipment required to connect contractor facilities to CMSNET or other CMS-chosen network.
7. Work with other CMS contractors to support and troubleshoot all points of integration to ensure they remain operational and are improved as necessary. Activities within the scope of integration include:
  - a. Provide on-going analysis of source systems to determine the timeliness, accuracy, consistency, and granularity of the source data to be extracted; determine how derived or consolidated data shall be created and verified; determine the best possible source for each data element;
  - b. Integrate data from multiple data sources with integrity and consistency;
  - c. Review existing ETL routines and propose enhancements as needed;
  - d. Develop and maintain design of interfaces to all required internal and external data sources;
  - e. Provide integration support to other CMS initiatives as needed;
  - f. Plan for continued phased implementation/deployment of the NDW Production environment;
  - g. Adhere to CMS directed change and configuration management policies and service level management processes;
  - h. Address data feed changes on an as-needed basis via the Change Control process.

8. Implement a comprehensive QA plan to ensure the accuracy of data feeds and reports.
9. Proactively analyze and detect potential data quality problems throughout the entire process of acquiring, maintaining, reporting and archiving NDW data.
10. Implement a data quality solution with the goal of delivering comprehensive, consistent, relevant, and timely data to NDW end users regardless of its application, use, or origin.
11. Design a mechanism, compliant with CMS VDC design, to support the daily transfer of data source providers' files to the VDC Contractor.
12. Manage a metadata environment that ensures end users can efficiently find data elements, learn what they mean, understand where they come from, and how they are used. Overall goals include:
  - a. Improve efficiency and accuracy of analysis
  - b. Enterprise-wide understanding and proper usage of business terms
  - c. Central and consolidated metadata repository for end-users to find data definitions and perform analyses
13. Collaborate with the stakeholders to define and maintain a metadata dictionary and future reporting requirements.
14. Review existing metadata management strategies and propose enhancements as needed.
15. Capture, analyze, and manage a repository of business processes and business logic necessary to report and manage Contact Center Operations.
16. Optimize the logical and physical data models and the extract, transfer & load (ETL) workflows to eliminate redundant data and improve ETL, database and application performance.
17. Implement changes to support Next Generation Desktop (NGD) releases. Specifically, the contractor shall work with the NGD data provider to understand the impact of planned changes to the NGD source data feed on the NDW. The contractor shall undertake the required development efforts to incorporate these source data changes into the NDW and work with the UAT contractor to validate report output using test data housed within the NDW contractor's environment.
18. Implement changes to support multiple Intelligent Voice Responses (IVRs) with separate periodic releases. The contractor shall work with the source for IVR data to understand the impact of planned changes to the IVR source data feed on the NDW. The contractor shall undertake the required development efforts necessary to incorporate these source data changes into the NDW.
19. Continue the development of the NDW. Major development activities include, but may not be limited to:
  - a. Reviewing, and updating as needed, all relevant design-related documents;
  - b. Reviewing, and updating as needed, documentation of NDW environments (Development, Test, UAT, and Production);
  - c. Reviewing, and updating as needed, all relevant Standard Operating Procedures (SOPs);
  - d. Proactively suggesting improvements for the NDW operations;
  - e. Completing analysis white papers for CMS as requested (such as evaluations of industry best practices); assume one per quarter;
  - f. Ensuring that all activities conducted under the task order and all products delivered comply with CMS's security policy;
  - g. Ensuring that all products developed and delivered adhere to Health Insurance Portability and Accountability Act (HIPAA) compliance standards;

- h. Ensuring that all electronic information technology products developed or used to support the NDW are Section 508 compliant as required;
  - i. Complying with the CMS Technical Reference Architecture (TRA) requirements;
  - j. Reviewing existing logical and physical data models and proposing enhancements as needed;
  - k. Developing data mining and archive techniques that will ensure all historical data is captured and securely stored within the NDW environment;
  - l. Providing CMS detailed analysis and trending of the data;
  - m. Implementing data and reporting access data security plan;
  - n. Complying with CMS Change Management standards and policies for configuration management, change management, and release management;
  - o. In coordination with the CMS VDC Project Management Office (PMO) and in compliance with the CMS VDC policy and procedures, the NDW contractor shall have remote access to the production NDW environment in the VDC necessary to support NDW operations; and,
  - p. Identifying problems, recommending solutions, and communicating potential efficiencies and cost-effective improvements.
20. Continue the operations of the NDW. Major activities include, but may not be limited to:
- a. Working with VDC contractor to ensure necessary infrastructure is in place from contractor's location to remotely access, monitor, and maintain the NDW production environment. Access is currently accomplished via secure communications channel compliant with CMS Security requirements and CITRIX server or equivalent.
  - b. Supporting the VDC contractor to provide timely access to reliable data including the ability to merge all data related to contact center operations, desktop activities, all QA data, print fulfillment activities, reference center data, and all network data including IVR and TDD/TTY, routing, computer telephony integration (CTI) and desktop applications.
  - c. Supporting the VDC contractor's efforts to ensure uninterrupted access to data from the NDW by providing software support and application maintenance.
  - d. Supporting VDC contractor audits to ensure adherence to defined security plan.
  - e. Completing NDW Systems Manual defining procedures for data load monitoring and troubleshooting, supporting the VDC planning for database and application server disk use, restart and recovery, and escalation procedures.
  - f. Coordinating build release process and operational environment upgrades with CMS Data Center staff and the VDC.
21. Continue the maintenance of the NDW. Major activities include, but may not be limited to:
- a. Maintaining components of the NDW Development, Test, and UAT environments including, software and sample/test data feeds.
  - b. Providing ongoing storage requirements and growth factors that are used to monitor and expand the NDW Storage Area Network (SAN).
  - c. Conducting software upgrades as required in Development, Test and UAT.
  - d. Maintaining comprehensive, documented testing procedures.
  - e. In coordination with the NDW VDC contractor, monitoring and managing preventive maintenance of all NDW application components.



22. Coordinate with CMS to determine and propose a CMS-tailored solution for reporting on contact center operations and key performance indicators. The solution shall cover a range of methodologies including an intelligent dashboard, standard reports, multi-dimensional “slice-and-dice” functionality, and ad-hoc capabilities. All aspects of the reporting solution shall be fully integrated within the overall end-user reporting solution, made available to CMS staff and other selected contractors, and be focused on key areas that could determine areas of potential improvement and operational efficiencies within the CCO.
23. Create and maintain a Reporting Plan document that outlines the reporting solution proposed for the period of performance. Work with CMS to develop and maintain an inventory of reports produced by the NDW.
24. Monitor and evaluate reports currently produced manually by the user community to provide recommendations to CMS about adding additional automated reports to the schedule.
25. Make all new reports accessible to the NDW user community with the BI tool(s) in the NDW Production environment utilizing appropriate security measures.
26. Maintain the NDW to ensure the successful creation of all Medicare and Marketplace Telecom and NGD Reports. These reports provide CMS with an overview of contact center operations for the previous day.
27. Support ad-hoc reporting requests from CMS and contact center contractors.
28. Create a standardized Ad-hoc Report Request Form that can be used by CMS and other contractors to submit their requests electronically to the NDW.
29. Provide NDW user support to CMS and contractor staff by developing, operating, and maintaining an efficient Helpdesk. Support shall also be provided through training materials developed, delivered, and periodically updated by the contractor.
30. Develop and implement the methodology to be used throughout the lifecycle of a help desk ticket from initial capture of issue through to resolution.
31. Implement a custom-built or COTS application to be utilized in logging, tracking and resolving help desk tickets. Provide monthly reports generated from the tracking system and list Open, Closed and In Progress Help Desk tickets.
32. Develop and maintain frequently asked questions (FAQs) to be accessible to end-users through the Web-enabled reporting tool and other CMS Internet sites as required by CMS.
33. Provide, organize, maintain, and disseminate all NDW training materials.
34. Develop and maintain a plan for alternative training approaches including Internet-based (ex. Utilizing WebEx) or video-teleconference training, and Computer Based Training (CBT) programs that could be distributed to users for completion at their convenience.
35. Manage timelines, communications, human resources, costs, quality, and risk. The contractor shall report on how the work is being accomplished and scheduled, including the activities of any subcontractor(s).
36. Allow full access into all related facilities (including data centers or other support locations), at any time during normal operating hours, to CMS employees or persons designated by CMS.

## **B. Security:**

The contractor shall comply with the applicable security requirements related to the operation of NDW defined in the Business Partner System Security Manual (BPSSM) (also known as IOM Publication 100-17), the Core Security Requirements and its operational appendices (A, B and C), found at <http://www.cms.gov/Manuals/IOM/>. The contractor shall implement a security program that adheres to CMS security standards.

The CMS Information Security Library can be found here:

<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

The contractor shall fully cooperate with CMS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities. The following security regulations, policies, and guidelines are applicable to all CMS contractors:

1. Public Law 93-579, The Privacy Act of 1974, as amended
2. Public Law 99-474, Computer Fraud & Abuse Act of 1986
3. Public Law 100-235, Computer Security Act of 1987
4. Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35
5. Public Law 104-106, Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act)
6. Public Law 104-191, Health Insurance Portability and Accountability Act, 1996 (formerly known as the Kennedy-Kassenbaum Act)
7. Public Law 107-347, E-Government Act of 2002, Federal Information Systems Management Act (FISMA)
8. Presidential Decision Directive/NSC-63 (PDD 63), Critical Infrastructure Protection, May 22, 1998
9. Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control, June 21, 1995
10. OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000
11. Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000
12. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999
13. CMS Business Partners System Security Manual, March 5, 2004
14. CMS Information System Security Policy, Standards and Guidelines handbook (The Handbook), version 1.2, July 19, 2004
15. CMS System Security Plan Methodology, version 3.0, November 6, 2002
16. CMS Risk Assessment Methodology, version 2.1, April 22, 2005